...making excellence a habit.™

ISO/IEC 27001 Information Security Management System (ISMS) for the aerospace industry

The aerospace industry is undergoing huge growth and rapid digital transformation. Flight safety and security have always been of paramount importance and the industry has historically had a good security record and reputation. However, digitalization and the adoption of emerging technologies have increased the risk of information and cybersecurity threats.

The sheer volume of data (be it personal information on pilots and passengers, or in relation to maintenance, flight information, and weather systems) continues to grow. Accompanied by the need for users to access the data remotely, and via multiple systems, there is the added dependence on data and connectivity, leading to increased risk of attack. And that's where ISO/IEC 27001 can help.

What is ISO/IEC 27001?

Internationally recognized, ISO/IEC 27001 is a framework which helps organizations manage and protect their information assets so that they remain safe and secure. It helps you continually review and refine the way you do this, not only for today, but also for the future.

The ability to manage information safely and securely has never been more important. ISO/IEC 27001 not only helps protect your business, but it also sends a clear signal to customers, suppliers, and the market place that your organization has the ability to handle information securely.

ISO/IEC 27001 is a robust framework that helps you ensure confidentiality, integrity, and availability of information, such as financial data, intellectual property, or sensitive customer information. It helps you identify risks and put in place appropriate security measures to manage them. So ISO/IEC 27001 not only protects your business, but your reputation, too.

Privacy spotlight

If your organization is processing large quantities of data, ISO/IEC 27701 Privacy Information Management System (PIMS), provides guidance on the protection of privacy and helps address an increasing number of regulations such as GDPR and CCPA.

Continuity spotlight

If responding to cyber-attacks, data breaches or technology outages is a concern for you or your suppliers, ISO 22301 provides a common framework to help you plan and prepare in case the worst happens.

Cybersecurity spotlight

If cybersecurity risks are a focus for your organization, you can build upon the ISO/IEC 27001 framework with complementary services from BSI, including penetration testing and NIST.

How ISO/IEC 27001 complements the AS EN 9100-series

Due to the ISO high level structure, ISO/IEC 27001 aligns to the new AS EN 9100-series, meaning that if you already hold AS EN 9100-series certification, you're in a good position to start the process of integrating information security into your Aerospace Quality Management System. Having complementary management systems allows organizations to anticipate, adapt, and respond to the risks and opportunities created by a highly competitive, innovative industry like aerospace. This provides organizations, large and small, with the resilience and agility needed to thrive in the global market.

The IAQG (International Aerospace Quality Group) makes reference to a number of information security and cybersecurity requirements in the AS EN 9100-series standard. Clause 7.5.3.1 states the following:

"Documented information required by the quality management system and by this International Standard shall be controlled to ensure:

- it is available and suitable for use, where and when it is needed
- it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity)"[1]

There are further references throughout the standard, including clause 8.1 on 'Operational planning and control' which refers to personal safety (which could include blackmail and ID theft), product safety (which can apply to the purchase and development of software and firmware), the prevention and detection of foreign objects (for example malware), and the establishment of controls (this could apply to software and firmware). A non-conformance could be a built-in vulnerability.

Industry recommendations on information and cybersecurity

In addition to the IAQG AS EN 9100-series of standards, the European Centre for Cybersecurity in Aviation (ECCSA) has made a number of recommendations in relation to aviation cybersecurity, including:

> "Aviation industry organizations should obtain the highest-level executive sponsorship within their business and establish a governing integrity framework to address product cybersecurity." [Paragraph 3.2.a]

> "Aviation industry organizations should define a product cybersecurity policy and appoint a dedicated product cybersecurity leader responsible for implementing and maintaining an effective product cybersecurity program within their organization." [Paragraph 3.2.2][2]

Furthermore, the AIA (Aerospace Industries Association) Civil Aviation Cybersecurity Industry Assessment and Recommendations Report states that:

> "Working collaboratively, all stakeholders need to strive to establish a common cybersecurity trust framework that includes a governance structure and technology standards that quantify the minimum expectations for cybersecurity, methods of mutual trust, and a common understanding of interoperable risk acceptance. Stakeholders must then proactively identify, understand and prioritize the risks to aviation systems in order to mitigate them."[3]

And beyond the AS EN 9100-series, other aerospace standards which require evidence of compliance with information security and cybersecurity requirements include AS EN 9115. This deals with the relationship between information assurance, information security, and cybersecurity, as well as the Aircraft Data Network, the Aviation Industry Standards for Digital Information Security, the Commercial Aircraft Information Security Concepts of Operation, and Process Framework and Datalink Security.

How ISO/IEC 27001 benefits organizations

ISO/IEC 27001 will help organizations across the industry sector, large and small, manage a range of information and cybersecurity risks. More specifically:

- Travel agents handle large volumes of passenger data and therefore face the threat of cyber attack
- Airports face the risk of leaked passenger personal data and movement information, compromised security surveillance systems, customs and passport control, border services, homeland defence, and air traffic control. Understanding such data flows and ensuring appropriate management is where ISO/IEC 27001 provides best practice structure
- Airline operators also face the threat of passenger data attack on big data live streaming services, communications, and WiFi. Evaluating, prioritizing, and responding to the risk these pose is required by ISO/IEC 27001
- Manufacturers and MROs (maintenance, repair and overhaul) need to consider the security of their in-house systems, research and development facilities, externally purchased hardware, firmware and software, the 5G revolution in relation to predictive maintenance and intelligent services, and test equipment. With 114 different security controls in ISO/IEC 27001, there is a toolset available to help minimize the risk to an acceptable level for your organization

Regardless of the products and services you offer, it's also critical to ensure contractual, regulatory, or Governmental obligations to keep clients' data secure are met. This is particularly prominent in military and defence where there are specific regulations, including Cybersecurity Maturity Model Certification (CMMC) administered by the Department of Defense (DoD) in the US, requirements stipulated by the Ministry of Defence (MoD) in the UK, and equivalent requirements in other countries.

Aerospace vulnerabilities

In recent years, there have been numerous high profile examples of aerospace organizations falling foul to data breaches, in turn negatively impacting reputation and customer perceptions.

In 2016, the US Department of Homeland Security revealed that it had successfully hacked a Boeing 757 airliner on the runway.[4] And in the last twelve months, nearly 8,000 unique and verified software vulnerabilities were disclosed in the US National Vulnerability Database.[5]

Other examples of the potential for data vulnerabilities arising from the adoption of new technology applications in aerospace include electronic flight bags (EFBs), In Flight Entertainment (IFE), and Crew Wireless Services.

Commenting on a high profile passenger data breach in the sector in 2018, a spokesperson from the Information Commissioner's Office in the UK said: "... the law is clear - when you are entrusted with personal data, you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."[6]

So it's clear to see that the stakes are high and the risks will only continue to rise. Proactively managing your information security with ISO/IEC 27001 will help you better protect your customers, staff, brand reputation, and business performance.

1. AS EN 9100-series Standard
2. European Centre for Cybersecurity in Aviation (ECCSA) Recommendations
3. AIA (Aerospace Industries Association) Civil Aviation Cybersecurity Industry Assessment & Recommendations Report. (August 2019)
4. Tripwire. (November 2017). A Boeing 757 was hacked remotely while it sat on the runway
5. Info Security Magazine. (February 2018). 7900 Vulnerabilities Didn't Make It into the CVE Database in 2017
6. BBC News. (July 2019). British Airways faces record £183m fine for data breach

Other ISO/IEC 27001 benefits include:

- Improved reputation and stakeholder confidence
- Better visibility of risk amongst interested parties
- Enhanced trust and credibility in the market to help you win more business
- Reduced likelihood of fines or prosecution
- Assistance in remaining compliant with relevant legislation
- Improved information security awareness amongst all relevant parties
- Reduced likelihood of staff-related information security breaches
- Demonstration of commitment to information security at all levels of the business
- Increased organizational resilience
- Reduced costs through minimizing incidents

Simplifying trade across boundaries:

As many organizations in the aerospace supply chain operate or trade internationally, working to ISO/IEC 27001 will simplify trade across boundaries, whether geographic, political, economic, commercial, or social. Simplification and standardization can give you that competitive edge in the market.

What steps do I need to take?

To start your journey to ISO/IEC 27001 certification, follow these steps:

- Purchase a copy of the standard from BSI and read it
- Make sure you have buy-in from your leadership team
- Book a training course with BSI to understand the requirements of the standard. (BSI offers everything from Requirements of ISO/IEC 27001:2013 to Information Security Management Systems Auditor/ Lead Auditor Training)
- Identify organizational gaps which need to be addressed to meet the new requirements
- Develop an implementation plan
- Liaise with your local BSI office for further help and support

About BSI in Aerospace

By Royal Charter

The aerospace industry demands quality at every stage – and is underpinned by stringent requirements for safety and reliability. From assessment, certification and training to software solutions, advisory services and supply chain intelligence, BSI provides the full solution to facilitate business improvement and help aerospace clients drive performance, manage risk and grow sustainably.

Today, BSI leads the way in exploring best practice for Smart Cities, Internet of Things, Unmanned aircraft vehicles, and digital manufacturing – enabling aerospace organizations to be better equipped when facing the challenges of tomorrow.

Find out more about ISO/IEC 27001, visit **bsigroup.com/en-NZ**

BSI/NZ/1683/SC/1219/EN/GRP